UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/926,460	01/28/2002	Oliver Richter	RICH30001/JEK	4672

23364 7590 02/24/2005

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2683	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/926,460	RICHTER, OLIVER	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 11-04-04 have been fully considered but they are not persuasive.

1. The applicant's amendment overcomes the examiner's previous objections.

2. The applicant's amendment, in the examiner's view, broadens the claims and therefore is still rejected by the same prior art for the reasons below.

3. The applicant argues Schroderus fails to not only disclose and suggest control of the first use of mobile equipment and the deactivation of an additional application after receiving a confirmation signal, but Schroderus clearly fails to describe providing a request for confirmation whether it is indeed a first use of the mobile equipment. The examiner disagrees – Kenagy is used to remedy the deficiency since he discloses a first-time user must call the service provider to obtain a temporary password. The ability of the network to validate the user and give them said temporary password is the "confirmation" that the user has been authenticated and reads on the claim.

4. The applicant argues that Kenagy does not use a SIM card. While this is true, Kenagy is used to remedy the deficiency of Schroderus who did not disclose a "first use authentication" operation, as Kenagy does. Hence, Kenagy discloses authentication via use of the network while Schroderus would use this same operation to consult the SIM card. Teachings of a "first use" are taught by Kenagy as interpreted by the examiner in his office action (also see #3 above). Kenagy allows use of two passwords, ie. the temporary password and the new password which would be generated by the user (as is known in the art). Lastly, it is the examiner's interpretation from Kenagy's teachings that a first use operation is performed once (to give a temporary password) whereby all subsequent operations would use a new, user-generated password (again, which is well known in the art).

5. It appears that the applicant argues the validity of the combination of the prior art of record (see letter "c", page 13). The examiner's Office Action clearly shows prior art from the same field of endeavor which solve similar problems. The use of Kenagy's

teachings, albeit "different" from Schroderus, remedy the situation by providing teachings that ultimately read on the applicant's claims. Hence the combination is valid and correct.

6. The applicant argues the prior art does not reject claim 9. The examiner disagrees since Brogan teaches all the components disclosed by the applicant and Kenagy teaches a SIM/smart card that runs an application (on the smart card) the first time the phone is used to corroborate a temporar/entered PIN with a stored password (abstract and figure 4a, #202, #204, #206 and #208). The examiner interprets the "stored password" as being stored in a "protected area" of memory such that a user cannot access it and thus fraudulently use the phone. Hence, Kenagy remedies the deficiencies of Brogan's apparatus.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4 and 7 rejected under 35 U.S.C. 103(a) as being unpatentable over Schroderus et al. US 5,907,804 and further in view of Kenagy et al. US 5,842,124 (hereafter Schroderus and Kenagy).

As per **claim 1**, Schroderus teaches a method for putting into operation a processor smart card in a network for communication, ~~for example a GSM network~~ wherein the card user ~~must identify himself~~ is identifiedwith respect to the processor smart card (SIM) by a PIN (title, abstract, figure 1 and C1, L48-58 teaches GSM SIM card), comprising the steps of:

For execution control of its use, the processor smart card is first provided ~~by the card manufacturer or card personalizer~~ with an additional application, ~~preferably the SIM Application Toolkit, which prevents its~~ arranged to prevent use in the network,

instead allowing only local use by means of a card reader or card terminal, ~~preferably a mobile phone device~~ (figure 1 shows that the phone is prevented from outgoing communications unless a valid PIN is entered, see steps #103, #105 and #106), and

Upon the use of the processor smart card, the application outputs without a further check of a secret number a display signal for the use and a request for confirmation (figure 1, step #102 requests a PIN code), and

But is silent on control of its first use AND after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled.

The examiner interprets Schroderus' operation in figure 1 as reading on the operation of putting a processor smart card into operation since both require the SIM card to validate a PIN number entered by the user AND both prevent normal operation of the phone when a valid PIN is not entered.

Kenagy teaches a manual process whereby the user, on a first use of the phone, calls a service provider to obtain a temporary password which is input to gain access to the network (abstract, figures 1-2 and 4a, #202, #204, #206, #208, C8, L37-63). The examiner notes that this operation of calling the service provider is ONLY performed once and the phone will be so changed as to not require the "temporary password" upon further use which therefore reads on the claims.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Kenagy, such a special algorithm is run during control of its first use AND after receiving a confirmation signal the additional application is deactivated or its execution so changed that upon the next use of the card a display signal is outputted to indicate that the card has already been put into operation and the use of the processor smart card in the network is enabled, to provide means for authenticating once such that the user does not have to perform this operation each time the phone is turned on (the examiner notes that many phones provide for a user-selectable option to require PIN authentication each time the phone is turned on for extra security).

As per **claim 2** Schroderus in view of Kenagy teaches claim1 wherein a PIN number previously defined, ~~preferably by the card manufacturer or card personalizer~~, must be inputted for activating the additional application (figure 1 teaches inputting a PIN code #102 which causes an application to validate said PIN and reads on activating the additional application).

As per **claim 3** Schroderus in view of Kenagy teaches claim 1 or 2 **but is silent on** wherein the entry of a PIN and/or secret number (PUK) for changing or unblocking the PIN is requested after the first use of the card and prior to the deactivation or change of state of the additional application.

Kenagy teachs inputting a temporary PIN (eg. supplied by the manufacturer or service provider) which will/can then be changed by the user to a more personal PIN number (as is well known) which reads on the claim (abstract, C11, L10-32).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Schroderus in view of Kenagy, such that entry of a PIN and/or secret number (PUK) for changing or unblocking the PIN is requested after the first use of the card and prior to the deactivation or change of state of the additional application, to provide means to re-verify the PIN/PUK so that the user can change the password (eg. enter it once and then re-verify it – this ensures the user has entered the PIN twice and correctly changed it and the phone can deactivate or change state of the additional application).

As per **claim 4** Schroderus in view of Kenagy teaches claim 1 or 2 **but is silent on** wherein <u>at least</u> some or all PIN numbers on the card ~~were already~~ <u>are predetermined and</u> personalized on the processor SIM ~~by the smart card manufacturer and~~ said numbers are indicated upon the first use for later use on the card reader or card terminal, ~~prefereably a mobile phone device.~~

Kenagy teaches the manufacturer or service provider can preprogram the SIM with PIN numbers (C11, L10-32).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Schroderus in view of Kenagy, such that some/all of the PIN numbers on the card were already personalized on the processor SIM by the smart card manufacturer and said numbers are indicated upon the first use for later use on the card reader or card terminal, prefereably a mobile phone device, to provide means for the manufacturer to pre-program a temporary PIN into the phone which the user verifies on the first use.

As per **claim 7** Schroderus in view of Kenagy teaches claim 1 wherein the secret numbers to be defined at the first putting into operation are used not for the purpose of protecting the network application but for protecting an additional application, ~~preferably a SIM application toolkit application, on the SIM~~ on the smart card.

Claim 5 rejected under 35 U.S.C. 103(a) as being unpatentable over Schroderus and Kenagy as applied to claim 1 and further in view of Hopkins US 5,757,918 (hereafter Hopkins).

As per **claim 5** Schroderus in view of Kenagy teaches claim 1 wherein some or all PIN numbers on the card are set by a random-number generator built into the card and said numbers are indicated during the first use on the card reader or terminal, ~~preferably a mobile phone device.~~

Hopkins teaches A method for granting or denying access based upon the verification of a user and authentication of a smart card and using a random number generator contained within the smart card to generate a random number (see claim 1).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Schroderus in view of Kenagy, such that the SIM card has a built-in random-number generator, so that it can generate random number PINs that would be used by the phone user and changed from time-to-time to increase security.

Claims 6 and 8 rejected under 35 U.S.C. 103(a) as being unpatentable over Schroderus and Kenagy as applied to claim 1 and further in view of Davis et al. US 6,314,519 (hereafter Davis).

As per **claim 6** Schroderus in view of Kenagy teaches claim 1 **but is silent on** wherein some ~~or all~~ PIN numbers are combined for transmission to the network, ~~prefereably~~ in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator or network service provider.

The examiner notes that this function is well known in the art – eg. computer systems routinely require users to change their logon passwords periodically which requires the user to, in essence, change the password and transmit it back to the server for storage in a PIN database. The password is encrypted for security. – Hence, as per claim 1, Kenagy teaches changing the temporary PIN to a user-selected PIN which may require transmittal back to the service provider. Further to this point is **Davis**, whereby there are secured electronic (financial) transactions are based on a peer-to-peer closed loop system in which the sending party generates a secure transaction that comprises a value amount (eg. PIN) and an authentication code. In order to establish and complete a transaction, the requesting party inserts uses a Smart Card and enters an identification code. The transaction processing system authenticates the Smart Card (eg. via a PIN database). While Davis focuses mainly on financial transactions, one skilled would use the same secure operations for PIN change updates (C17, L51 to 18, L-16).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Schroderus in view of Kenagy, such that wherein some or all PIN numbers are combined for transmission to the network, prefereably in encrypted form via a data channel, and sent immediately or at a later time to a central place at the network operator/provider, to provide means for the operator to have/store the latest PIN changes/updates as made by the user thus ensuring they can be correctly authenticated.

As per **claim 8** Schroderus in view of Kenagy teaches claim 1 **but is silent on** wherein the information on the first use of the processor smart card and on the PIN numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal ~~or preferably the mobile phone device.~~

Davis teaches an RF/Cellular system (figure 1) and hardware which supports a user selected personal identification number that is programmed into the Smart Card via the subscriber unit or pager, thus disabling access to any features of the protected Smart Card unless subsequently accessed or reprogrammed by the subscriber unit or pager (C3, L10-16) AND The message entry device 1018 allows a user to initiate a cash load request, cash transaction, credit transaction, or the like. Typically, a user might enter a request using a keyboard, a **voice activated recognition device**, a touch-sensitive device (e.g., screen or pad), or other convenient data entry device (C18, L16-21 teaches voice recognition data input).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Schroderus in view of Kenagy, such that information on the first use of the processor smart card and on the PIN numbers is outputted or inputted via the hearing or speaking devices of the card reader, the card terminal or preferably the mobile phone device, to provide means for hands-free entering of data (and reception of PIN data via speaker too).

Claim 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Brogan et al. US 6,012,634 Kenagy (hereafter Brogan).

As per **claim 9**, Brogan teaches a smart card (figure 4, #400) comprising a microprocessor (#402), memory area (#404 and #412) and an interface each connected to the microprocessor (figure 4 shows all components connected to the microprocessor via "interfaces" as well as ports #408 and #414 - whereby the microprocessor/memory inherently store software programs/data that support operation of the phone and supporting user applications) **but is silent on** and further comprising a memory area where an application for the execution control of the first use of the smart card is stored

and a secret memory area where the information on the first use of the smart card is stored ~~data on said application are stored in protected fashion.~~

Kenagy teaches a SIM/smart card that runs an application (on the smart card) the first time the phone is used to corroborate a temporary/entered PIN with a stored password (abstract and figure 4a, #202, #204, #206 and #208). The examiner interprets the "stored password" as being stored in a "protected area" of memory such that a user cannot access it and thus fraudulently use the phone.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify Brogan, such that the smart card comprises a memory area where an application for the execution control of the first use of the smart card is stored and a secret memory area where data on said application are stored in protected fashion, to provide means to run an authentication program the first time the phone is turned on which requires a PIN to be entered that matches a stored PIN to ensure a person is not fraudulently using the phone.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 703-306-5426. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 703-308-5318. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Stephen D'Agosta
PRIMARY EXAMINER
2-22-05